STATE OF WEST VIRGINIA
OFFICE OF THE ATTORNEY GENERAL
DARRELL V. MCGRAW, JR.
CONSUMER PROTECTION DIVISION
1-800-368-8808 or 304-558-8986

Press Release

FOR IMMEDIATE RELEASE

April 18, 2008

Contact: Douglas L. Davis
Phone: (304) 558-8986

Attorney General McGraw Warns Members of WVU Employee's Federal Credit Union of Email Phishing Scam

Attorney General Darrell McGraw is warning members of the West Virginia University Employee's Federal Credit Union about an email phishing scam being sent to members of the credit union. Some members have reported receiving automated telephone calls as well.

Specifically, the phoney emails and phone calls advise credit union members that their accounts have been frozen due to fraud and that they must call a telephone number in order to regain access to their accounts. When members dial the number given in the email or on the robocalls, the automated answering machine requests members to input their account numbers or debit card numbers along with their personal identification numbers. The message then advises that the account has been reactivated and hangs up. According to the West Virginia Employee's Federal Credit Union and the West Virginia University Police, three people have been victimized by the scam and within minutes of providing their account numbers, a total of $4,000.00 was taken from their credit union accounts and transferred to an account in Pakistan.

After being alerted to the scam, Attorney General McGraw's Consumer Protection Division was successful in getting three of the fraudulent phone numbers disconnected by working with the local telephone service providers hosting the fraudulent phone numbers.

"No bank or financial institution will send you an email asking you to call a bogus phone number where you will have to provide confidential information such as your account number or Social Security number," Attorney General McGraw warned. "If your financial institution needs some sort of action from you, they will send you a letter in the mail or call you and ask you to come in."

This phishing scam is a little different than most. In typical phishing scams, crooks will design a website to look like a legitimate website and send an email claiming to be from a bank or credit union, instructing the recipient to click on a link to visit the website. The reasons given for receiving the bogus email ranges from fraud to security updates and identity verification. When victims visit the bogus websites, it appears as though they are at the legitimate websites of their financial institutions and are sometimes lured into giving personal financial information including account numbers and Social Security numbers.

"Any time you receive a communication from your bank or credit union, call the telephone number listed on your monthly statement, or better yet, visit in person," said Attorney General McGraw.

If you have been a victim of fraud and need the assistance of the Attorney General's office, please contact the Consumer

Protection Division, toll-free at 1-800-368-8808 or visit Attorney General McGraw's website at www.wvago.gov.

##